HARDWARE SPOOFER SETUP GUIDE

1. Prepare the Bootable USB with BIOS:

- Create a Windows bootable USB using a tool like **Rufus** or **Windows Media Creation** Tool.
- Download the **latest BIOS** version for your specific motherboard model from the manufacturer's website.
- Save this BIOS file onto the same USB drive containing the Windows bootable image.

2. Backup Current Hardware IDs:

- Run the **Hardware Checker** tool to retrieve your current hardware IDs.
- Save a copy of these IDs for later comparison after spoofing.

3. Plug in the TPM Chip and Update BIOS:

- Install the **TPM (Trusted Platform Module) chip** securely onto your motherboard.
- Boot up and enter the **BIOS/UEFI settings** (usually by pressing **Delete** or **F2** during startup).
- Update your motherboard BIOS using the file saved on the USB drive. Your PC will **automatically restart** once the process is finished.

4. Configure BIOS Settings for Secure Boot:

- In the BIOS, set the **Boot Mode** to **UEFI** (Unified Extensible Firmware Interface).
- Navigate to **Secure Boot** settings, then select **Clear all Secure Boot keys** to reset them.
- Reinstall the Secure Boot keys as required, then **Save and Exit** to apply the changes.

5. Install Windows from the USB:

- **Boot** from the Windows bootable USB to start the installation.
- For privacy and to avoid tracking, choose to set up an **offline account** rather than a Microsoft account during installation.

6. Run the Hardware Spoofer Tool:

- Ensure **Windows Defender** and any other antivirus software are fully disabled to prevent any interference with the spoofing process.
- For **Windows 11**, **Memory Integrity** must be disabled for the spoofing process. To do this, open the **Hardware Checker** tool, press and hold **ALT**, then press the letter **D** three times. The system will automatically restart, and Memory Integrity will be disabled.
- Open the **Hardware Spoofer** tool, allow the tool to complete the spoofing process. Your PC will **automatically restart** once the process is finished.

7. Verify Changes in Hardware IDs:

- After restarting, run the **Hardware Checker** tool again.
- **Compare** the new hardware IDs with your saved backup to confirm that the spoofing process was successful.
- After completing the spoofing process, you can re-enable **Memory Integrity** if desired. Press and hold **ALT**, then press the letter **E** three times. The system will automatically restart, and Memory Integrity will be re-enabled.

Note: *The TPM ID will only change if you replace the TPM chip.*

🔓 Password To Extract The Files : **7RkxXUiDBT92t7qbheA7**